2022 Second International Conference on Interdisciplinary Cyber Physical Systems (ICPS) | 978-1-6654-7022-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICPS55917.2022.00046

Development of Cyber Attack Model for Private Network

Mostafa Al-Amin
Computer Science & Engineering
Jagannath University
Dhaka, Bangladesh
masharif46@yahoo.com

Mirza Akhi Khatun
Computer Science & Engineering
Jagannath University
Dhaka, Bangladesh
mirza_akhi@hotmail.com

Mohammed Nasir Uddin
Computer Science & Engineering
Jagannath University
Dhaka, Bangladesh
uddinmn@mail.ru

***Abstract*—Cyber Attack is the most challenging issue all over the world. Nowadays, Cyber-attacks are increasing on digital systems and organizations. Innovation and utilization of new digital technology, infrastructure, connectivity, and dependency on digital strategies are transforming day by day. The cyber threat scope has extended significantly. Currently, attackers are becoming more sophisticated, well-organized, and professional in generating malware programs in Python, C Programming, C++ Programming, Java, SQL, PHP, JavaScript, Ruby etc. Accurate attack modeling techniques provide cyber-attack planning, which can be applied quickly during a different ongoing cyber-attack. This paper aims to create a new cyber-attack model that will extend the existing model, which provides a better understanding of the network's vulnerabilities.**

Moreover, It helps protect the company or private network infrastructure from future cyber-attacks. The final goal is to handle cyber-attacks efficacious manner using attack modeling techniques. Nowadays, many organizations, companies, authorities, industries, and individuals have faced cybercrime. To execute attacks using our model where honeypot, the firewall, DMZ and any other security are available in any environment.

***Keywords*-Cyber Attack, Cyber Threat, Network Threat, Honeypot, Firewalls, DMZ, Backdoor, Payload, Python, Network Vulnerabilities, Private Network, LAN.**

I. Introduction

Mainly computer technology and detailed technology solutions have significantly enhanced the infrastructures of civilization and our economy [1]. The vulnerability to computer technology increases more harm while cyber-security increases, as per the Symantec cybercrime report, published in April 2012 [2]. Day by day, cyber-security is becoming steadily perspective since the users manipulate computer networks extends.

Many cyber security specialists believe that malware is the familiar choice of arms to bring about malicious expects to crack cyber protection efforts in cyberspace [3]. Cyber-attack models detect network vulnerabilities that help protect networks from future attacks [4]. We have the best knowledge about cyber-attack and security that we have achieved and different books and publications. After the study, we found that the model is not enough for cyber-attack because antivirus, firewalls, honeypot, DMZ, and other security devices are available to prevent the attack. Currently, the devices are too much up to date. Unfortunately, the number of cyber-attack models is reasonably low, and even the previous models break to represent all the required properties of a cyber-attack [5]. So, we need to think of different models which will be simple to comprehend. However, we are going to propose a new model of cyber-attack. In this model, we will be able to attack the private network from the internet. Mainly our target employee, IT expert, system admin, but not a target machine directly the because target machine or server has much security such as firewall, DMZ, honeypot etc. The paper analyzes the present cyber-attack model for developing a cyber-attack model and bypassing major antivirus programs.

This cyber-attack model can constitute a cyberattack commonly and shortly with the growing popularity of online services. The paper analyzes various information about organizations, and industry, including the different types of event attacks. This presentation technique can be captured at many points, such as operating system access, access to a private network, backdoor creation, bypassing the primary antivirus, etc.

A. Research Motivation

The main objective of this study is to create a model of modern cyber-attack, which can identify any company's network infrastructural vulnerabilities and enable cyber security experts to solve their problems before being hacked and raise cyber awareness among company employees about cyber security.

There are some analyses of cyber-attack modeling techniques and cyber-attack security techniques In the current situation. We have identified that it has different techniques. All the methods provide interesting intuition about a cyber-attack [6]. Some papers state that they extend the model of cyber-attack much more influential. However, Various models are not capable of breaking the latest security system. Most of the time, to break the attack data might be located in honeypots at one-half of this addition [7]. The type of attack and the appropriate tools operate the attack data for analysis.

B. Contributions

In this work, we have proposed a strategy for developing cyber-attacks. We have created a real-time environment for designing attack models. By doing this, the contributions of this study are as follows:

978-1-6654-7022-3/22/$31.00 ©2022 IEEE
DOI 10.1109/ICPS55917.2022.00046

- Our proposed cyber-attack model depends on the private network to attack the system. It was the earliest endeavor to enter the system via a private network because there was no direct connection over the internet.
- We created the real-time scenario and attacked the system properly. Further, this scenario can be found in figure 1

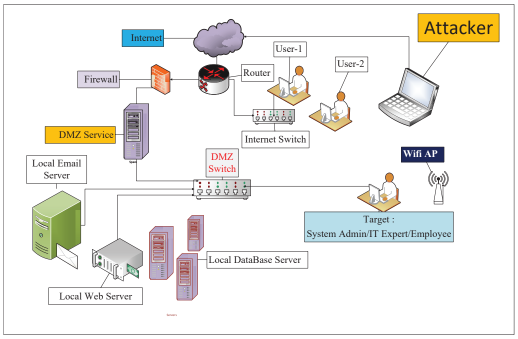


Fig. 1. Attack Scenario

- Our Data-Center was live and highly secured. We also gripped the server from the physical GEO location to obtain better performance in our proposed method.
- Our method is designed for different companies, organizations, and industries. We connected to the system using the target employees' information (e.g. IP addresses, Domain names, DNS information, Netblocks, companies' Websites, phone numbers, and social groups associated with a person's name). Therefore, based on this concept, we provided the details of our proposed cyber-attack model.

The roadmap for this work is arranged as follows: In part II, we narrate *event attacks* and the potential types of attack. Part III explores the related work on developing the cyber-attack model. We then described the presented methodology procedure to attack the system based on bypassing antivirus protection in part IV. We estimated the performances and discoursed our results in part V, and the last part of the paper concludes in part VI.

II. Event Attacks

In this part, we describe the various kinds of event attacks. Also, introduce a brief description of each attack that occurred on the target system. Our attacks represent the security problems exploited based on the communication model [8].

While developing event attacks, we focused on the local networks. For example, employees' data is crucial in the organization, and organizations' information on their systems is also confidential. In those cases, our first target will be the employees' information so that we can access the primary system via the employees' network. The work to date has recognized the different types of event attacks:

- **Domain Name server (DNS) Spoofing:** It keeps evidence of domains like a phonebook of the internet and goes with IP addresses. It exchanges the IP address through the domain names [9].
- **Sniffing:** This attack might be sniffing the network credential and scanning the data packets. A hacker sends a contracted aspect of the detail and keeps the data confidential. If the information is not perfectly encoded, it can be cracked open with a scan [10]. When the hacker is connected to the network by spoofing, next will try to detect and acquire the credentials like a password, e-mail, FTP, the database, etc [11].
- **Eavesdropping:** A malicious node can be monitored an incident that contains sensitive and confidential data. It is supposed to be just open to the specific components [8].
- **Malware:** It is a kind of malicious element that a hacker might employ on unauthorized occasions. Transporting the port forwarding variables as per strike holes all over the Network address translation and disclosing the assembled particular computers starts with forwarding GET requests to the system [12].
- **Collusion:** Rather than two malicious elements can be colluded to utilize the functionalities or resources of the target system [8].
- **Denial of Service (DoS) Attack:** A DoS attack is the type of attack that can be made a machine unavailable such as the user might not enter the system/network [13]. It blockades mega storage on the target system and focuses on rebooting the system or the network [11].
- **Ping of Death:** The mega ping packet will send to the target system to conduct down the system by attackers because of the requirement of the system's ability to keep up the mega ping packets [14].
- **Interception:** A malicious component can stop an event. It is supposed to be sent to other stuff and can be forwarded back inaccurate responses [8].
- **Phishing Mail Attacks:** Phishing defines as an attack technique through e-mail that is used to obtain user data and login credentials. Primarily, an attacker hides a malicious program into the e-mail, instant message, impersonating it, as usual, content for taking the detailed information from the victim. This attack might appeal to the networks and the whole computer platforms [15]–[19].

III. Related Work

This part provides the existing work of the proposed model. Several techniques for analyzing the cyber-attack include Attack Graph, Attack Vector, Attack Surface, Attack Tree, and Diamond Model [20]–[23]. Hamad *et al.* Described the three attacks modeling techniques called Kill Chain, Diamond Model, and Attack Graph for cyber-attack modeling. Nevertheless, the limitation was that no practical experiment was there to extract information for understanding the cyber-attacks.

Simeon *et al.* Proposed event-based applications and systems and explained the conditions of the security vulnerabilities. However, modern security solutions rely on code analysis, encryption, and other techniques. Nevertheless, this research has been the only technique approved to build the attack model [4].

Nabi *et al.* Introduced the incident attack simulation that used the Uppaal tool to framework the vulnerability but reused the design specification from the existing application [24].

Wagner *et al.* Presented a framework that pretends the system to connect with possible evaluation. The administrators of diverse network platforms intended for simulation and assessment in the defender frameworks concerning certified and uncertified hardware. The scenarios visualize the agent-based simulation approach [25].

IV. Proposed Method

We have proposed an advanced new cyber-attack model. The critical phenomenon of this model is to attack a private network in any organization or a system, which is entirely separate from the internet, but any user or system using the internet and the private network simultaneously.

The motivation for our approach is to create a concrete foundation for an attacker who will be able to attack an organization or system if they use both internet and private networks at the same time. The Block Diagram of the proposed model is as follows in Figure. 2

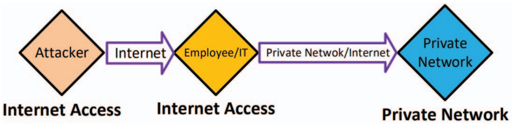


Fig. 2. Block Diagram Proposed Model

The traditional survey also needs to consider how the attacker can successfully exploit any vulnerability and the threats associated with each attack. Our proposed attack model includes the resulting pseudocode in Algorithm 1.

We believe that our new attack model can be possible to access any operating system, android phone, Linux, and iOS despite maximum security. This attack depends on how good is our delivery method because we have already bypassed 55 antivirus programs. The delivery method is most important for penetration testing.

A. Information Gathering

Footprinting is the method used for collecting information about computer systems and servers. To get victims' information, we used various types of technology, such as *Python*, *C Programming*, *C++ Programming*, *SQL*, *JavaScript*, *PHP*, *Java*, *Ruby* etc. To find out more about the companies' websites, IP addresses, Domain names, DNS names, Netblocks, and social groups associated with a person's name using Programming. First of all, we collect information from company employees on the Internet. So, there is another way to gather information about the employees when they visit social media such as Facebook and LinkedIn or any other social platform as they leave traces on the Internet.

Algorithm 1: Pseudocode for Cyber Attack Model

```
Data: Gathering Information
Result: Finally Attacked and Exploited
while Target is Not Found, do
    Start Gathering Information
      Target1 = Primary Target Employee
      Target2 = Amied Target
    Start Program to Attack = Target1  if Port
      Scanning is Success then
        Preparing Trojan Backdoor/Rootkit
    else
        $result$ → Start Scanning Another, Employee
    end
    if Sending Payload then
        Bypasss Anitvirus Program
    end
    if Successfully Delivery Payload to Target1 then
        Aimed to Target2
    else
        Try to Delivery Payload to Target1
    end
    if Successfully Delivery Payload to Target2 then
        Result → Attacked and Exploited
    else
        Result → Not Attacked
    end
end
```

B. Target

The main reason is to identify the target for entering the system. So, after getting all the information about the victim, we analyzed that the target system is highly secured with different security systems like a honeypot, DMZ, IDS & IPS, etc. We cannot connect directly to the target server due to DMZ or a private network. That is why we need to divide our attack process into the two-step. We selected two targets as the primary target and the aimed target. Target selection and attack plan are important to ensure a successful attack.

We planned another approach so that we do not miss any target. We did not find the email address of a few employees. For this reason, we take this step. We sent them various links through social media. When the employee clicked on those links, the payload was installed automatically on their computer.

C. Delivery

There are lots of delivery methods for passing backdoor to the target system. Nevertheless, we have seen specific ideas and scenarios to attack. After that, we selected the delivery method because the most common one is the email delivery method for all hackers. It also depends on what kind of information we have collected earlier. The easiest way to deliver a payload or virus is to send it via email. There is not a single method that can assure the accomplishment of the attack. Nevertheless, failure to attack sometimes is essential for getting basic credentials of the target system. The mechanisms of gathering information are ordinary in browser-based attacks. In that case, the user hits the malicious web page, which is the first attempt to obtain the necessary credential of the system, and we try to distribute the malware payload to the victim's computer. We have to select the delivery method based on the victim's movement. In our case, we select Email delivery to send the malicious backdoor/payload to the victim's computer. The victim has received this backdoor/payload and can no longer control this attacker's backdoor/payload until the victim executes the backdoor/payload. If the attacker does not execute this file, we need to send it again or try to find another distribution method.

D. Primary Target

In this step, we started our attack on the primary target. Since the computer devices propagated on the internet, that provides us with a way to hack as follows in Figure 1. We used the advanced IP scanner and another IP scanner to collect more accurate information. We scan the target network to see how many IPs they are using. Also, we found how many ports are open or closed in the target network.

E. Generating Backdoor

We need to generate a backdoor to access the primary target. So, there are several ways to create a backdoor. Here, we built a backdoor program in python. Inside that backdoor, we have all the information of the kali server so that when a victim clicks on this backdoor, a reserved TCP connection will be made with the server, and a terminal will open immediately. Then the attacker will have full access to the victim's computer. After getting access to the victim's computer or network, we can attack any computer or server connected locally to this victim's computer in the private network. Our main job is to send malware to these victims' servers or computers.

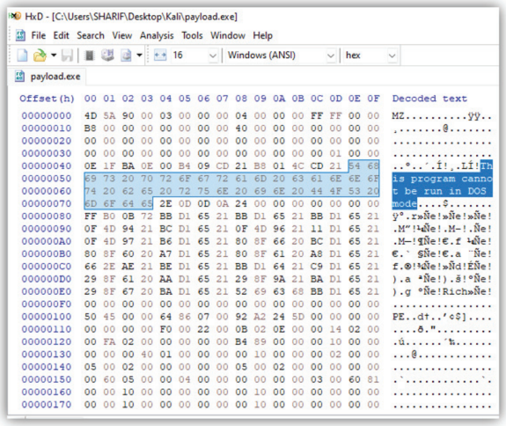
However, the problem is that the victim's computer allows them to update their antivirus regularly. That is why we can allow list malware on the victim's computer so that the malware works well after the antivirus update and the malware needs to be updated immediately. Frequently, we had to update this backdoor because the system updated day by day.

F. Bypass Antivirus Program

Antiviruses are a huge irritate for attackers. When an attacker needs to penetrate a system, the good or bad outcome relies on whether the prey system has installed the antivirus or not. However, bypass is usually the last major problem among attackers. Nonetheless, there is no reliable bulletproof strategy to bypass antivirus. However, depending on the current environment, we should try to apply all systems one by one. There are many ways to avoid antivirus programs, such as encoder, packer, binary editing, changing payload signatures, changing source code and changing payload versions.

If the attacker got the source code of the malware, then he can easily change it. For example, if there is an option to control the order in the system, turn it toward if-else. The functioning of the code should not influence any remarkable process. There are several changes that a hacker can edit, like upper to the lower case, changing parameters, Etc. *int target=0;* might be edited to *int TARGET=0;*

Antiviruses use file signatures to detect viruses. It is a unique pattern whose size is small as a few dozen bytes. It can detect the virus and, in some cases, remove viruses.


HxD - [C:\Users\SHARIF\Desktop\Kali\payload.exe]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
payload.exe

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  ................
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  FF B0 0B 72 BB D1 65 21 BB D1 65 21 BB D1 65 21  ÿ°.r»Ñe!»Ñe!»Ñe!
00000090  0F 4D 94 21 BC D1 65 21 0F 4D 96 21 11 D1 65 21  .M"!¼Ñe!.M–!.Ñe!
000000A0  0F 4D 97 21 B6 D1 65 21 80 8F 66 20 BC D1 65 21  .M—!¶Ñe!€.f ¼Ñe!
000000B0  80 8F 60 20 A7 D1 65 21 80 8F 61 20 A8 D1 65 21  €.` §Ñe!€.a ¨Ñe!
000000C0  66 2E AE 21 BE D1 65 21 BB D1 64 21 C9 D1 65 21  f.®!¾Ñe!»Ñd!ÉÑe!
000000D0  29 8F 61 20 AA D1 65 21 29 8F 9A 21 BA D1 65 21  ).a ªÑe!).š!ºÑe!
000000E0  29 8F 67 20 BA D1 65 21 52 69 63 68 BB D1 65 21  ).g ºÑe!Rich»Ñe!
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  50 45 00 00 64 86 07 00 92 A2 24 5D 00 00 00 00  PE..d†..'¢$]....
00000110  00 00 00 00 F0 00 22 00 0B 02 0E 00 00 14 02 00  ....ð.".........
00000120  00 FA 02 00 00 00 00 00 B4 89 00 00 00 10 00 00  .ú......´‰......
00000130  00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00  ...@............
00000140  05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00  ................
00000150  00 60 05 00 00 04 00 00 00 00 00 00 03 00 60 81  .`............`.
00000160  00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00  ................
00000170  00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00  ................
```

Fig. 3. Bypass Antivirus Program

when we generate backdoors that are not detectable by any antivirus programs, and sometimes two or more antivirus programs detected them. However, we have seen how to open the backdoor using a text editor and modify its code to bypass these programs.

The backdoor code will try to alter the signature file when an antivirus program scans it. The signature file will not look similar to other harmful files. The antivirus program will say this is a usual file if it seems unique. It does not have any malicious code. However, we used this technique in our proposed method.

We looked for a usual character for readable sentences or readable text. Therefore, we modified the characters for creating the signature file. It will allow us to bypass antivirus programs. We put random characters in here to make this code look different from antivirus programs. Nevertheless, we did not put more or fewer characters and always kept the same number of characters. In doing so, we were so careful not to overwrite any of the code. Hence, this modified code saves it.

We created the backdoor to bypass the antivirus. We will now open that backdoor/payload with Hex Editor. Open the backdoor/payload in Figure 3 using HxD [26]. With Hex Editor, we will make changes inside the backdoor/payload. If we change this value, there is no rule that antivirus will be able to detect it. So, we gradually change the value and test with antivirus to see if the antivirus can detect it or not. After trying this way, we were finally able to bypass 55 antiviruses.

G. Aimed Target

In this step, we get to access the aimed target of the organization. We installed some applications on the target computer. As a result, some applications send the information to our kali server. If we successfully send a backdoor/payload to the target, we install some software immediately, such as keylogger, DDoS attack software etc. If possible, disable antivirus software or add white list backdoor/payload.

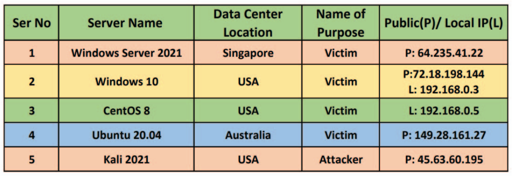
In addition, do a good audit of all computers as needed, such as based on what kind of work this victim's computer does and which software is utilized the most, and based on that, let us name the backdoor a similar name to that software. The victim does not realize that the computer has been hacked. Then modify the computer's registry and add a backdoor to the startup registry so that the computer can be rebooted and start backdoor automatically. Finally, we can attack their network through a variety of event attacks.

V. Performance & Evaluation

In this part, we decorate the result of our work and the percentage of event attacks with penetration testing of the proposed method.

A. Experimental Setup

This term, we used five servers like Windows 10, Ubuntu 20.04, Windows Server 2021, and CentOS 8, Kali Linux 2021. These servers are located in different geo-locations. We used the A + hosting Inc datacenter to do this penetration testing. Our servers are powered by VMware vSphere hypervisor. Each of our server configurations is four vCPU Core Intel Xeon E5 processors, 200 GB SSD storage & 8 GB RAM. The kali server, Windows 10, Ubuntu 20.04 & Windows server 2021 is connected to a 10 Gbps network port with a public IP address. The Centos 8 is connected to a local IP network. The list of IPs used in this attack model is given in the table 4.



Ser No	Server Name	Data Center Location	Name of Purpose	Public(P)/ Local IP(L)
1	Windows Server 2021	Singapore	Victim	P: 64.235.41.22
2	Windows 10	USA	Victim	P:72.18.198.144 L: 192.168.0.3
3	CentOS 8	USA	Victim	L: 192.168.0.5
4	Ubuntu 20.04	Australia	Victim	P: 149.28.161.27
5	Kali 2021	USA	Attacker	P: 45.63.60.195

Fig. 4. The List of IP

The actual physical location of Centos 8 and Windows 10 is USA Datacenter, Windows Server 2021 is Singapore Datacenter, and Ubuntu 20.04 is Australia Datacenter. we use this kali server as the attacker's computer. Windows Server 2021 and Ubuntu 20.04 are two computer victims. Mentionable that the virus definition of Microsoft Windows Defender is up to date, and the firewall is enabled. The experimental network setup is as follows in Figure 5.

B. Comparison

The standard traditional cyber-attack model cannot attack any private network, computer or server [5] [7] [10] because the private network is not directly connected to the internet. However, this model can be capable of striking any private network through a company's employee. We can make different types of attacks using this model, such as Ping of Death, DNS Spoofing, DoS Attack, Phishing Attack, Eavesdropping, Malware, and Sniffing. On the other hand, the traditional attack model cannot make the above attack because there is no direct connection in a private network from the internet. Hackers attack companies' private networks using an employee as a gateway. In most cases, as for any attack, we need to send payload .exe which is a ubiquitous method but essential for any Windows System.

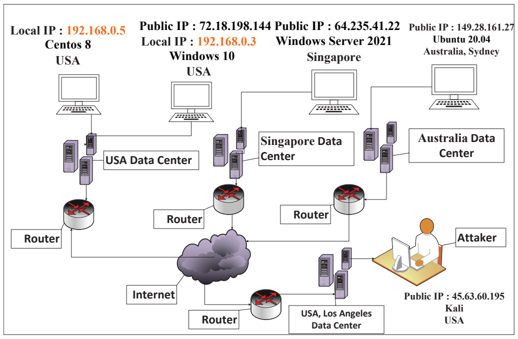
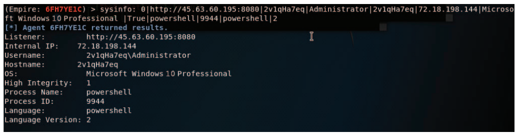


Fig. 5. Network Infrastructure Setup

C. Result & Discussion

This part illustrates the result and discussion of the proposed cyber-attack model and the respective analysis of the performance-related attack modeling with Kali Linux. We mentioned earlier that Kali Server IP 45.63.60.195 & Windows 10 target IP 72.18.198.144. Finally, we accessed the target system, as shown in figure 4. From this picture, it is understood that Windows 10 now has full computer access to Hacker. Windows 10 and Centos 8 are both connected to a private network. Now we can attack the private network computer because we already have access to the private network's computer . Figure 6.



```
(Empire: 6FH7YE1C) > sysinfo: 0|http://45.63.60.195:8080|2v1qHa7eq|Administrator|2v1qHa7eq|72.18.198.144|Microso
ft Windows 10 Professional |True|powershell|9944|powershell|2
[*] Agent 6FH7YE1C returned results.
Listener:         http://45.63.60.195:8080
Internal IP:    72.18.198.144
Username:         2v1qHa7eq\Administrator
Hostname:       2v1qHa7eq
OS:               Microsoft Windows 10 Professional
High Integrity:   1
Process Name:     powershell
Process ID:       9944
Language:         powershell
Language Version: 2
```

Fig. 6. Attacked to the Target Machine

In our attack model, we get the best performance for following the attacks, Ping of Death, DNS Spoofing, DoS Attack, Phishing Attack, Eavesdropping, Malware, Sniffing. Our proposed model got access to the Windows 10 operating system. The percentage of the attacks in our proposed method is shown in Figure 7.

Based on the potential attacks, figure 4 shows the percentage of attacks that occurred during Penetration Testing.

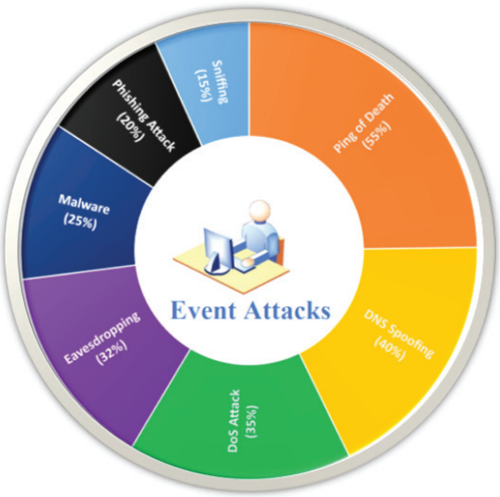


Fig. 7. Event Attacks, and the Percentage

VI. Conclusion

Cyber-attacks are growing every day. Attackers are smart enough to create new malware to access the system. Nowadays, small and big businesses have started using web portals or e-commerce websites. Even school students are immersed in the internet or computer [27]. So we all need to raise cyber awareness.

This paper presented a way of attacking computers and private networks. Moreover, through the attack model, we realized that the private network is not out of cyber-attack. So, we all have to be careful about using private networks and the internet. If a computer is hacked and this hacked computer is connected to a private network somehow, then the private network can be a victim of a cyber-attack.

However, the limitation of our model is that a company employee must be connected to a personal network and the internet at the same time. Otherwise, we cannot attack a private network. Nevertheless, we can attack any internet computer or server. Our aim is to extend the cyber-attack model more effectively.

References

[1] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014.

[2] M. Fossi, G. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, J. Blackbird, M. K. Low, D. Mazurek, D. McKinney *et al.*, "Symantec internet security threat report trends for 2010," *Volume XVI*, 2011.

[3] H. Ha, "Online security and consumer protection in ecommerce an australian case," in *Strategic and pragmatic e-business: Implications for future business practices*. IGI Global, 2012, pp. 217–243.

[4] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-attack modeling analysis techniques: An overview," in *2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW)*. IEEE, 2016, pp. 69–76.

[5] F. Chowdhury, "Modelling cyber attacks," *International Journal of Network Security & Its Applications (IJNSA) Vol*, vol. 9, 2017.

[6] M. Younas, I. Awan, and J. El Haddad, *4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. IEEE Computer Society, 2016.

[7] H. Al-Mohannadi, I. Awan, J. A. Hamar, A. Cullen, J. P. Disso, and L. Armitage, "Cyber threat intelligence from honeypot data using elasticsearch," *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, pp. 900–906, 2018.

[8] Y. K. Lee, D. Nam, and N. Medvidovic, "Identifying inter-component communication vulnerabilities in eventbased systems," Technical Report: USC-CSSE-17-801, Tech. Rep., 2016.

[9] N. Tripathi, M. Swarnkar, and N. Hubballi, "Dns spoofing in local networks made easy," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2017, pp. 1–6.

[10] P. Anu and S. Vimala, "A survey on sniffing attacks on computer networks," in *2017 International Conference on Intelligent Computing and Control (I2C2)*. IEEE, 2017, pp. 1–5.

[11] M. A. Khatun, N. Chowdhury, and M. N. Uddin, "Malicious nodes detection based on artificial neural network in iot environments," in *2019 22nd International Conference on Computer and Information Technology (ICCIT)*. IEEE, 2019, pp. 1–6.

[12] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2016, pp. 195–200.

[13] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[14] E. Gelenbe and Y. Yin, "Deep learning with dense random neural networks," in *International Conference on Man–Machine Interactions*. Springer, 2017, pp. 3–18.

[15] M. Adil, M. A. Almaiah, A. Omar Alsayed, and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, no. 8, p. 2311, 2020.

[16] A. K. Al Hwaitat, M. A. Almaiah, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, "Improved security particle swarm optimization (pso) algorithm to detect radio jamming attacks in mobile networks," *Quintana*, vol. 11, no. 4, pp. 614–624, 2020.

[17] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6461–6471, 2020.

[18] A. ALMAIAH and O. ALMOMANI, "An investigation of digital forensics for shamoon attack behaviour in fog computing and threat intelligence for incident response," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 07, 2020.

[19] ——, "An investigator digital forensics frequencies particle swarm optimization for dectection and classification of apt attack in fog computing enviroment (idf-fpso)," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 07, 2020.

[20] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, and E. Weippl, "Dark clouds on the horizon: Using cloud storage as attack vector and online slack space," 2011.

[21] P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371–386, 2010.

[22] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," Center For Cyber Intelligence Analysis and Threat Research Hanover Md, Tech. Rep., 2013.

[23] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proceedings of the 1998 workshop on New security paradigms*, 1998, pp. 71–79.

[24] F. Nabi, J. Yong, and X. Tao, "A novel approach for component based application logic event attack modeling." *Int. J. Netw. Secur.*, vol. 22, no. 3, pp. 435–441, 2020.

[25] N. Wagner, R. Lippmann, M. Winterrose, J. Riordan, T. Yu, and W. W. Streilein, "Agent-based simulation for assessing network security risk due to unauthorized hardware," in *Proceedings of the Symposium on Agent-Directed Simulation*, 2015, pp. 18–26.

[26] M. Hörz, "Hxd-freeware hex editor and disk editor," 2008.

[27] P. K. Nalla, R. K. Gajavelly, J. Baumgartner, H. Mony, R. Kanzelman, and A. Ivrii, "The art of semi-formal bug hunting," in *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2016, pp. 1–8.